Hendry County Sheriff’s Office

General Order 5.11

TITLE: FCIC/NCIC/CJNET and use of DAVID	**SHERIFF’S APPROVAL:** Digital
ORIGINATION DATE: March 18, 2019	**REVISION DATE:** May 14, 2019
RELATED REFERENCES: *Criminal Information Services Security Policy, §119 F.S.* **CFA:** *26.03*	
REVIEW FREQUENCY: 3 YEARS	**DATE OF NEXT REVIEW:** May 14, 2022

I. **PURPOSE:** To ensure the proper use of any and all services provided by the Florida Crime Information Center (FCIC) and its links to the National Crime Information Center (NCIC) and the Criminal Justice Network (CJNET). Standard operating procedures have been established in order to provide for the entry, validation, auditing, dissemination, retention, removal and security pertaining to privileged information and its related data, as addressed by Ch.119 FSS (i.e. Florida public records laws), Ch. 943 FSS (Department of Law Enforcement) and Chapter 11C-6 and 11C-8 of the identification manual issued by the Florida Department of Law Enforcement (FDLE).

II. **SCOPE:** This order shall apply to all sheriff’s office members.

III. **POLICY:** It is the policy of the Hendry County Sheriff’s Office to maintain the integrity of the NCIC/FCIC and CJNET systems through FDLE guidelines and comply with Department of Highway Safety and Motor Vehicles (DHSMV) Memorandum of Understanding (MOU) for the use of DAVID. The Hendry County Sheriff’s Office will follow the Criminal Justice Information Services (CJIS) security policy (CSP) in effect.

IV. **PROCEDURE:**

Criminal Justice Information Services

A. The CJI system, and information obtained from the system, may only be used by criminal justice personal for criminal justice purposes in compliance with NCIC rules and regulations, operations manuals, and state and federal laws. Information obtained from CJI files, or computer interfaces to other State or Federal systems shall only be used for criminal justice purposes by criminal justice personnel in compliance with rules, regulations, and state and federal laws.(CSP 4.3)

1. Hendry County members shall ensure that access to the system is for authorized criminal justice purposes, or for purposes authorized by State or Federal law and shall regulate proper use at all times.

2. HCSO members authorized to use, view, or obtain information from the FCIC/NCIC system shall receive and maintain their user certification by taking either the Limited Access or Full Access FCIC/NCIC Certification training and pass the corresponding exam.

3. HCSO shall enforce the policies for information handling and protection also applies to using CJI shared with or received from FBI CJIS for non criminal justice purposes. A noncriminal justice purpose includes the use of criminal history records for purposes authorized by federal or state law other than purposes relating to the administration of criminal justice, including - but not limited to - employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances. (CSP 5.1.1.1.)

4. The HCSO shall validate the dissemination of CJI to an authorized recipient. For validation process HCSO shall refer to the information exchange agreement. (CSP 5.1.1)

5. Hendry County members who violate CJI access rules and regulations, disclose information to unauthorized individuals, or violate any other CJI rules, regulations, or procedures will be subject to discipline up to and including dismissal, as stated in HCSO policy. (CSP 5.12.4)

6. Questions regarding the use of the system or problems related to these systems should be directed to the FCIC Agency Coordinator (FAC) or alternate FAC's.

7. The CJIS Certification Guide produced by the Florida Department of Law Enforcement shall be referenced by members to ensure that all required policies and procedures are being followed.

B. Physical Security

1. Information Technology (IT) Director shall serve as the FCIC/NCIC security officer (ISO) to ensure the security of CJI workstations.

2. The Information Technology Division shall be responsible for the secure connection of Hendry County workstations to FCIC.

3. Hardware, software, and, media, including laptops, shall be located in a physically secure location when being used to access the FCIC/NCIC system. A "physically secure location" is a facility, an area, a room, a group of rooms, server room, wiring closets or a police vehicle under the management control/security of Hendry County Sheriff Office personnel. A deputy's residence is not necessarily considered a "secure location" if the system can be viewed by others. (CSP 5.9 & CSP 5.8)

4. All HCSO secured locations are behind locked doors and access is restricted to authorized personnel. Access is approved by administrative staff thru the Chief Deputy.

5. Each terminal operator shall have his/her own password and user code. The user code will be issued by the FCIC Agency Coordinator. Passwords and user codes shall be kept confidential and not shared with other agency members.

6. Workstation operators shall always log off at the end of their shift or whenever another operator wants to use the system.

7. The operator shall log off any time they are not in control of that workstation.

8. The HCSO shall take measures to prevent multiple concurrent active sessions for one user identification, for those applications accessing CJI, unless the agency grants authority based upon operational business needs. Agencies shall document the parameters of the operational business needs for multiple concurrent active sessions. The HCSO shall ensure that only authorized personnel can add, change, or remove component devices, dial-up connections and remove or alter programs. (CSP 5.5.2.2)

9. The monitor shall not be visible to unauthorized persons.

10. HCSO members shall accompany all visitors to computer centers and/or workstation areas at all times.

11. A personally owned information system (BYOD- Bring your own device) shall not be authorized to access, process, store or transmit CJI. (CSP 5.5.6.1)

C. Media Protection

1. No CJI may be removed from secured location and/or departmental authorized equipment. This media protection prohibits transfer of CJI to unauthorized individuals. (CSP 5.8)

2. Data backup shall be kept in a secured location in an electronic format. Physical media for archival purpose shall be stored in a secured location. (CSP 5.8)

3. In the event that any electronic or physical CJI media needs to be transported outside of secured locations, this media must be transported by CJIS certified personnel. (CSP 5.8)

4. The agency shall sanitize, that is, overwrite at least three times or degauss electronic media prior to disposal or release for use by unauthorized individuals. (CSP 5.8.3)

5. Inoperable electronic media shall be destroyed (cut up, shredded, etc.) (CSP 5.8.3)

6. The HCSO shall maintain written documentation of the steps taken to sanitize or destroy electronic media. (CSP 5.8.3)

7. Agencies shall ensure the sanitization or destruction is witnessed or carried out by IT department. (CSP 5.8.3)

D. Security Incident

1. Any threat or perceived threat should be documented on a Security Incident Response Form and promptly forwarded up the chain of command to FAC, CAC (CJIS Agency Coordinator and LASO. The CAC and ISO will then forward to FDLE Customer support center. (CSP 5.3, Appendix F, FDLE CJNet ISO Resource Page)

    a. The Security Incident Response Form shall be maintained with the IT Director for a minimum of 3 years.

    b. The ISO shall be designated point of contact (POC) on all security related Issues. (CSP 5.3)

2. The Hendry County Sheriff Office has software in place for both network and client security to proactively prevent a security incident occurring. If a security incident occurs, notice will be sent via email to ISO. The incident will be immediately logged and updated in the security software. (CSP 5.10.4.5(3) Appendix E) (Appendix F FDLE CJNET ISO Resource page)

    a. The HCSO LASO will notify agency personnel when made aware of security advisories or alerts. Notifications are at the discretion of the ISO. (CSP 5.10.4.5 & CSP 5.3)

E. Remote Access

1. The Hendry County Sheriff Office shall authorize, monitor, and control all methods of remote access to the information system. If access is allowed by IT Director then documentation of rationale shall be obtained and maintained for a period of three years. (CSP 5.5.6)

F. Wireless Protocols

1. The Hendry County Sheriff Office has established usage restrictions and implementation guidance for wireless technologies; and (ii) authorize, monitor, control wireless access to the information system. (CSP 5.5.7)

2. The HCSO shall grant wireless access based on trouble shooting or privileged functions purposed.

   a. The HCSO will enable logging where supported and review the logs on a recurring basis. At a minimum logs shall be reviewed monthly. (CSP 5.5.7.1 (13))

   b. The HCSO has enabled wireless features to include cryptographic authentication, firewalls and other privacy features (CSP 5.5.7.1(9))

   c. The HCSO shall ensure that encryption sizes are at least 128-bits and the default shared keys are replaced by unique keys (CSP 5.5.7.1(10)).

   d. The HCSO shall ensure that ad hoc mode has been disabled or IT Director has assessed the risk and it is tolerable. (CSP 5.5.7.1(11))

G. Authentication Strategy

1. The Hendry County Sheriff Office shall have mechanisms or processes that verify users are valid once they are uniquely identified. Each individual's identity shall be authenticated at the local agency level. (CSP 5.6.2)

2. HCSO utilizes biometric technology to comply with CJIS advanced authentication requirements.

H. Patch Management

1. The Hendry County Sheriff Office identifies and enforces patch management for all critical and security related patches. All CJIS facing systems are patched at least monthly to include:

   a. Testing of appropriate patches before installation.

   b. Rollback capabilities when installing patches, updates, etc.

   c. Automatic updates without individual user intervention.

   d. Centralized patch management.

   e. Patch requirements discovered during security assessments, continuous monitoring, or indicated response activity shall be addressed expeditiously. (CSP 5.10.4.1)

2. The HCSO shall employ virus protection mechanisms to detect and eradicate malicious codes at critical points throughout the network. The HCSO shall ensure malicious code protection in enabled at all critical points. (CSP 5.10.4.2)

I. Spam and Spyware

1. The HCSO shall have and implemented Spam and Spyware protection to detect and take appropriate action on unsolicited messages and spyware/adware and employ these spam protection mechanisms at critical information system entry points, workstations, servers, and MDT's respectively transported by electronic mail and attachments, internet access, and removable media. (CSP 5.10.4.3)

2. The HCSO shall receive, send, document, and react to, as needed, for all alerts and will be addressed and disseminated by LASO.

J. Lost or Stolen Devices

1. User must notify agency when a device is lost or stolen by emailing to

ITissues@hendrysheriff.org

2. The HCSO will lock and wipe a lost and/or stolen phone.

3. The HCSO will use advanced authentication (AA) waiver on laptops.

COMPUTERIZED CRIMINAL HISTORY (CCH)

A. Any member receiving a request for criminal history record information must ensure that the person making the request is authorized to receive the information. (CSP 5.1.1.1)

1. Members receiving criminal histories shall comply with all rules and regulations.

2. Any questions regarding the dissemination of criminal histories shall be directed to the FCIC Agency Coordinator. (CSP 5.1.1)

B. Criminal history record information may only be used for the purpose for which it was originally obtained.

C. Requests for criminal history information from non-criminal justice agencies for noncriminal justice purposes should be directed to the Florida Department of Law Enforcement.

D. A dissemination log of state or federal criminal history information shall be maintained for each query.

E. This record shall reflect:

1. Name, Race, Sex, and DOB.

2. The FBI or state identification number (SID) or other numeric identifiers, if applicable.

3. The purpose code for the criminal history.

4. The justification for the criminal history, such as case number

5. The person requesting the criminal history or who the criminal history was released to

6. The requesting agency

7. The release date

8. The operator who ran the criminal history.

9. **NOTE:** This log shall be maintained for at least four years after the date of inquiry and must be available for FCIC/NCIC audit purposes.

F. Data retention, dissemination and destruction:

1. Criminal History data shall not be retained in case files when the case is closed or the record is superseded.

2. Criminal History data must be shredded when members are finished with the information.

DRIVER AND VEHICLE INFORMATION DATABASE (DAVID)

A. The Sheriff has signed a Memorandum of Understanding (MOU) with the Florida Department of Highway Safety and Motor Vehicles (DHSMV) for access to the Driver and Vehicle Information Database (DAVID).

1. Information obtained from DAVID can only be disclosed to persons to whom disclosure is authorized under Florida law (section 119.0712(2), Florida Statutes) and federal law (Driver's Privacy Protection Act, 18 U.S.C. s. 2721-2725).

2. Unauthorized disclosure is not only a violation of this policy, but may also subject the violator to criminal and civil penalties.

3. Employees are also reminded that Emergency Contact Information (ECI) listed in DAVID is to be used only in emergencies.

a. Emergency contact information shall only be used for the purpose of notifying a person's registered contact in the event of a serious injury, death or other incapacitation. ECI shall not be released or utilized for ANY other purpose, including developing leads or for criminal investigative purposes.

4. Employees are reminded that accessing **any** members' DAVID records other than as required for an ongoing law enforcement incident or investigation or other law enforcement purpose is prohibited, as is any personal use.

5. Should any supervisor become aware that a subordinate has misused personal information obtained from the DAVID system, he or she shall make immediate notification to Administration via chain of command and the DAVID point of contact (POC).

a. The DAVID POC is responsible for notifying the DHSMV of the violation and following their instructions regarding notification to the individual whose personal information has been compromised.

(1) An agency-approved letter for this purpose is on file with the DAVID POC and in the Professional Standards Unit.

(2) The notification to DHSMV must include a brief summary of the incident, the date, number of records affected, and information regarding the notification of the affected individual, their name and names of personnel responsible, the corrective actions and date of actions completed.

6. The DAVID POC is responsible for sending a letter to the affected individual immediately following the determination that personal information had been compromised by unauthorized access on the DAVID system by the employee. A copy of the letter will be kept on file in the Professional Standards Unit.

7. Per DHSMV, DAVID photos ARE permitted to be used in photo line-ups for law enforcement investigations when all other alternatives have been exhausted.

8. Quarterly Quality Control Review Report:

a. Report completed each quarter by the POC to monitor compliance with the agreement. This report must be completed, utilizing Attachment II, Quarterly Quality Control Review Report, within 10 days after the end of each quarter and maintained for two years. The following must be included in the Quarterly Quality Control Review Report.

(1) A comparison of the DAVID users by agency report with the agency user list.

(2) A listing of any new or inactivated users since the last quarterly quality control review; and

(3) Documentation verifying that usage has been internally monitored to ensure proper, authorized use and dissemination.Therefore, use of the DAVID system is subject to documented monthly random reviews by the agency POC.

9. The POC is responsible for immediately inactivating user access/permissions following termination or the determination of negligent, improper or unauthorized use or dissemination of information. POC must update user access/permissions upon reassignment of users within five (5) business work days.

10. Annual Certification Statement: The POC shall submit to the DHSMV an annual statement indicating that the agency has evaluated and certifies that it has adequate controls in place to protect the personal data from unauthorized access, distribution, use, modification or disclosure and is in full compliance with the requirements of the agreement/MOU. The POC shall submit this statement annually, **within 45 days** after the anniversary of the MOU, which is **March 9**. (NOTE: During any year in which a Field Audit is conducted, submission of the Internal Control Attestation may satisfy the requirement to submit an Annual Control Certification Statement.)

11. Because personal data associated with a driver or motor vehicle record is protected under both federal and state law, and because driver license photographs and social security numbers are highly protected, **DHSMV strongly recommends that users not copy and paste data from DAVID into other documents or systems.**

a. Information retrieved from DAVID shall not be cut, pasted or attached into CAD or CTS.

(1) CTS users are permitted to transfer DHSMV data retrieved via FCIC into CTS reports as per current protocol.

12. Access to DAVID information is a resource for law enforcement purposes only. The Department of Highway Safety and Motor Vehicles (D.H.S.M.V.) remains the custodian of the DAVID information as related to public records requests and disclosure.

13. Any breach of security shall be reported to the DAVID POC and may be grounds for disciplinary action up to and including termination.

V. GLOSSARY

LOCAL WARRANT CHECK– An active warrant check of local Hendry County files.

BOLO AUTHORITY/RESPONSIBILITY – Deputy who requests a BOLO issued to coincide with the written report of an incident.

FIREARMS ELIGIBILITY SYSTEM (FES) - FES is a law enforcement Criminal Justice Information System. The goal of FES is to provide information of individuals who are prohibited by state and Federal law from purchasing or possessing firearms.

FLORIDA CRIME INFORMATION CENTER (FCIC) - FCIC is Florida's law enforcement/criminal justice information system. The goal of FCIC is to help the criminal justice community perform its duties by providing and maintaining a computerized filing system of accurate and timely documented criminal justice information.

NATIONAL CRIME INFORMATION CENTER (NCIC) - NCIC is a nationwide computerized information system established as a service to all criminal justice agencies – local, state and federal. FCIC is linked to NCIC to ensure that Florida law enforcement agencies have access to national files.

NATIONAL LAW ENFORCEMENT TELECOMMUNICATION SYSTEM (NLETS) -NLETS is the high-speed message switching system that routes all messages to out of–state law enforcement agencies.

CRIMINAL JUSTICE NETWORK (CJNet) - CJNet is a secure Intranet designed for use by the Florida criminal justice community.

CRIMINAL JUSTICE INFORMATION (CJI) - Information collected by criminal justice agencies that is needed for the performance of their legally authorized required functions.

CJIS Agency Coordinator (CAC) – The CJIS Agency Coordinator will act as the central point of contact regarding all communications between FDLE CJIS and the User Agency. The CAC will assist FDLE in helping facilitate discussions regarding CJIS matters between the User Agency and FDLE.

DRIVER AND VEHICLE INFORMATION DATABASE - The Department of Highway Safety and Motor Vehicles provides law enforcement access to retrieve driver and vehicle information for law enforcement purposes only.

FCIC AGENCY COORDINATOR (FAC) – The FCIC Agency Coordinator ensures compliance with the Legal and Policy Requirements contained within the CJIS User Agreement, and facilitates communication between FDLE CJIS and the User Agency regarding FCIC related matters. The Telecommunications Section Supervisor shall serve as the FCIC Agency Coordinator.

PERSONALLY IDENTIFIABLE INFORMATION (PII) - Information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. (CSP 4.3).

REMOTE ACCESS - Any temporary access to an agency's information system by a user (or an information system) communicating temporarily through an external, non-agency-controlled network. (e.g. the Internet).

ADMINISTRATION OF CRIMINAL JUSTICE - Performing functions of detection, apprehension, detention, pretrial release, post-trial release, prosecution, adjudication, correctional supervision, or rehabilitation of accused persons or criminal offenders by governmental agencies. The administration of criminal justice includes criminal identification activities and the collection, processing, storage, and dissemination of criminal justice information by governmental agencies.

Your electronic signature in Power DMS acknowledges you have read this policy and understand it.